ABSTRACT

A voting server transmits a list of plaintext and encrypted voting data obtained by encrypting the plaintext to a voter terminal, and the voter terminal transmits a selected encrypted candidate name corresponding to the plaintext elected by the voter to an encryption server. The encryption server returns encrypted voting data obtained by re-encrypting the encrypted candidate name to the voter terminal, and the voter terminal transmits the encrypted voting data received from the encryption server for voting. Decryption of the encrypted voting data is performed by an anonymous decryption system. The voter terminal certifies the voter to an authentication server, and affixes a digital signature to the encrypted voting data based on a common-key authentication base, transmitting the same to the voting server.